

Application No.: 10/648,770  
Amendment dated:  
After Final Office Action of September 6, 2007

Docket No.: 27592-00454-US

*Remarks*

Applicant thanks the Examiner for his consideration of this application. Applicant now requests reconsideration of this application in view of the above amendments and the remarks below.

Upon entry of the above amendments, Claims 1-16 and 33-46 will be pending in the application. Claims 1-4, 6, 7, 11, 33, and 38 will have been amended, and Claims 17-32 will have been canceled without prejudice. Claims 42-46 will have been added.

Applicant gratefully acknowledges the indication of allowable subject matter in Claims 16 and 32, at pages 12-13 of the Office Action.

At pages 5-6, the Office Action rejects Claims 1-32 under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement. Claims 17-32 have been canceled, rendering their rejections moot. The remaining rejections are respectfully traversed for at least the following reasons.

The Office Action asserts that the specification, at paragraphs 40-48, present a situation in which the public and private keys must be the same and further asserts that it is well-known in cryptography that these keys must be different to have a functioning system. There are at least two problems with these assertions.

First, the system still functions, even if the public and private keys are exactly the same. This may or may not be a useful system, but it is a working system, and one of ordinary skill in the art would certainly be able to make and use it. This, alone, is sufficient for enablement.

However, second, the specification at paragraphs 40-48 is not intended to provide exact details because, as noted in the Office Action, such details *are* well-known in the art of

cryptography. The equations and discussion are merely presented as a brief discussion of the operations of these well-known methods. Typically, the public key and private key will be different, and the “random value” sent with the digitally-signed message may be, for example, some value related to the digital signature (e.g., DS1) created using the private key and such that, when combined with the public key using an appropriate cryptographic function, will result in a digital signature (e.g., DS2), that should be equal to the digital signature transmitted with the message if the message is authentic. That is, the random value sent with the digital signature using the private key may or may not be the same as the random value used to compute the digital signature. Furthermore, the particular function used to generate the digital signature of the message (i.e., the one based on the private key) may not be exactly the same as the one used to compute the digital signature at the destination (i.e., the one based on the private key), as long as various mathematical properties are satisfied.

For at least these reasons, Applicant respectfully submits that the claims are enabled and requests withdrawal of these rejections.

At pages 6-8, the Office Action rejects Claims 1-3, 5, 6, 17-19, 21, 22, 33-35, and 37-40 under 35 U.S.C. § 102(b) as being anticipated by Moy (“RFC 2328 – OSPF Version 2”). At page 8, the Office Action rejects Claims 1-6, 17-22, 33-35, and 37-40 under 35 U.S.C. § 102(b) as being anticipated by Murphy et al. (“Digital Signature Protection of the OSPF Routing Protocol”). At pages 8-10, the Office Action rejects Claims 1-8, 10-12, 17-24, 26-28, and 33-41 under 35 U.S.C. § 102(b) as being anticipated by Nguyen et al. (U.S. Patent Application Publication No. 2002/0016926). At pages 10-11, the Office Action rejects Claims 13-15 and 29-31 under 35 U.S.C. § 103(a) as being unpatentable over the combination of Nguyen et al. with

Srivastava et al. (U.S. Patent No. 7,103,185). At page 12, the Office Action rejects Claims 9 and 35 under 35 U.S.C. § 103(a) as being unpatentable over the combination of Nguyen et al. with Srivastava et al., and further in view of Kaliski, Jr. (U.S. Patent No. 6,085,320). The rejections of Claims 17-31 are moot in view of their cancellation. The remaining rejections are respectfully traversed for at least the following reasons.

Applicant has amended independent Claims 1, 33, and 38 to clarify differences between the claimed invention and the cited references. In particular, Claim 1 now recites, among other things, “providing a specific multicast channel for sending jump-start messages by the nodes to said other nodes when a node has not received any regular start-up messages from other nodes on one or more multicast channels used for regular start-up messages” and “sending a jump-start message on said specific multicast channel from a start node that has not received any regular start-up messages, wherein the jump-start message is secured by the start node and the start node starts an operation or an application.” Claim 33 now recites, among other things, “wherein the node is configured to: send a start message on a specific multicast channel of a system when the node starts an operation or an application and when the node has not received regular start-up messages from other nodes on other multicast channels, wherein the start message is to be secured by the node.” Claim 38 now recites, “A method, comprising: sending, by a node in a system including at least one multicast channel on which the node can send multicast messages to other nodes, a start message on a specific multicast channel of the system when the node starts an operation or an application and when the node has not received regular start-up messages from other nodes on other multicast channels, wherein the start message is secured by the node.”

The Office Action, in the various rejections, relies upon the regular multicast channels and regular start-up protocol messages (e.g., hello messages) of the OSPF routing protocol as corresponding to the claimed specific multicast channel and the start message in the claims, prior to amendment. However, it is respectfully submitted that the claims have now been amended to clarify that they are directed to a specific multicast channel to be used for other start-up messages that are to be used when the regular start-up messages have not been received. This is supported by the specification, e.g., at paragraphs 32-43. It is respectfully submitted that, in view of these amendments, the cited references fail to disclose or suggest the claimed invention, either individually or in combination, and that, therefore, Claims 1-16 and 33-46 are allowable over the cited references.

Applicant has also added new Claims 42-46, where Claims 42-44 specify that the regular start-up messages are directed to "Hello Protocol" messages or Link State advertisement messages (e.g., as discussed at paragraph 32), and Claims 45 and 46 specify that the nodes in their respective parent claims comprise router nodes (supported in various locations throughout the specification). It is respectfully submitted that these claims are allowable for at least the same reasons as noted above with respect to their parent claims.

Applicant has not presented all possible arguments or may not have refuted the characterizations of either the claims or the prior art as may be found in the Office Action. However, the lack of such arguments or refutations is not intended to act as a waiver of such arguments or as concurrence with such characterizations.

Application No.: 10/648,770

Docket No.: 27592-00454-US

Amendment dated:

After Final Office Action of September 6, 2007

**Conclusion**

Applicant believes that the above amendments and remarks address all of the grounds for objection and rejection and place the application in condition for allowance. Applicant, therefore, respectfully requests favorable consideration of this response and reconsideration of this application.

If the Examiner believes, for any reason, that a personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided below.

Respectfully submitted,

Date: November 8, 2007



Jeffrey W. Gluck, Ph.D.

Registration No.: 44,457

CONNOLLY BOVE LODGE & HUTZ LLP

1875 Eye Street, NW

Suite 1100

Washington, DC 20006

Tel.: (202) 331-7111

Direct Dial: (202) 572-0322

Fax: (202) 293-6229